# 分散システムにおけるシステム資源へのアクセスのセキュリティ制御の方法およびシステム



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平9－251425

(43)公開日　平成９年(1997)９月22日

| (51)Int.Cl.[6] | | 識別記号 | 庁内整理番号 | ＦＩ | | 技術表示箇所 |
|---|---|---|---|---|---|---|
| Ｇ０６Ｆ | 12/14 | ３１０ | | Ｇ０６Ｆ | 12/14 | ３１０Ｋ |
| | 1/00 | ３７０ | | | 1/00 | ３７０Ｅ |
| | 12/00 | ５３７ | | | 12/00 | ５３７Ａ |
| | 13/00 | ３５１ | | | 13/00 | ３５１Ｅ |
| | 17/21 | | 7259－5Ｊ | Ｇ０９Ｃ | 1/00 | ６６０Ｅ |

審査請求　未請求　請求項の数22　ＦＤ　（全 14 頁）　最終頁に続く

(21)出願番号　特願平8－234642

(22)出願日　平成８年(1996)８月19日

(31)優先権主張番号　０８／５１６６７１

(32)優先日　1995年８月18日

(33)優先権主張国　米国（ＵＳ）

(71)出願人　591064003
サン・マイクロシステムズ・インコーポレーテッド
SUN MICROSYSTEMS, INCORPORATED
アメリカ合衆国　94043　カリフォルニア州・マウンテンビュー・ガルシア　アヴェニュウ・2550

(72)発明者　ダニー・エム・ネセット
アメリカ合衆国　94555　カリフォルニア州・フレモント・ウォパッシュ　リバープレイス・34810

(74)代理人　弁理士　山川　政樹

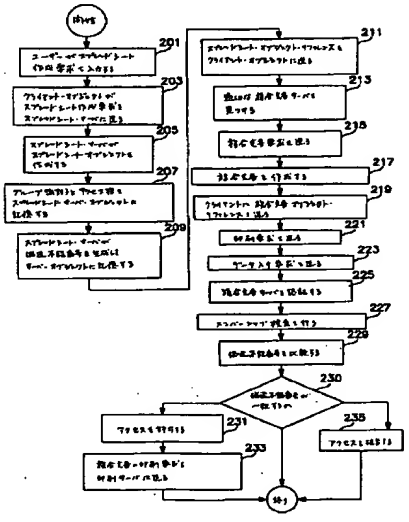
最終頁に続く

(54)【発明の名称】　分散システムにおけるシステム資源へのアクセスのセキュリティ制御の方法およびシステム

(57)【要約】

【課題】　分散コンピュータ・システム内の資源へのアクセスを安全に制御する改良された方法およびシステムを提供する。

【解決手段】　グループ識別標識を記憶し、それをターゲット・オブジェクトに結びつけ、次にメンバーシップ検査を使用して、ターゲット・オブジェクトへのアクセスを要求するクライアント・オブジェクトが、そのターゲット・オブジェクトに対するアクセス権を有するグループのメンバーであるか否かを判断する。このようにして、本発明は、要求側オブジェクトのアクセス権を検証するために、ある種の従来技術のシステムで一般的に行われていたようなコストのかかる暗号操作を省く。



【特許請求の範囲】

【請求項１】　コンピュータ・システムにおいて分散コンピュータ・システム内のシステム資源へのアクセスを制御する方法であって、
スプレッドシート・オブジェクトにグループ識別子を結びつけるためにクライアント・オブジェクトからスプレッドシート・サーバに要求を送るステップと、
スプレッドシート・サーバの制御下で、
スプレッドシート・オブジェクトを入手するステップと、
グループ識別子をスプレッドシート・オブジェクトと共に記憶するステップと、
偽造不能なチェックサムを生成するステップと、
偽造不能なチェックサムをスプレッドシート・オブジェクトと共に記憶するステップと、
偽造不能なチェックサムをクライアント・オブジェクトに送るステップと、
クライアント・オブジェクトの制御下で、
複合文書サーバに対して複合文書を印刷する要求を送るステップと、
複合文書サーバの制御下で、
グループ識別子と偽造不能チェックサムとを含む要求をスプレッドシート・サーバに送って、スプレッドシート・サーバがスプレッドシート・オブジェクトからデータを送り戻すように要求するステップと、
スプレッドシート・サーバの制御下で、
グループ識別子の解析に基づいてスプレッドシート・オブジェクトへのアクセスを許可または拒否するステップとを含む方法。

【請求項２】　分散コンピュータ・システムがクライアント・オブジェクトと、第１のサーバ・オブジェクトと、ターゲット・オブジェクトと、第２のサーバ・オブジェクトとを備え、それらの各オブジェクトがコンピュータ・システム内にあるオブジェクトの１つまたは複数の指定されたグループに属している場合に、分散コンピュータ・システム内のシステム資源へのアクセス制御を容易にするために、コンピュータ・システムにおいて実行される方法であって、
第１のサーバ・オブジェクトの制御下で、
ターゲット・オブジェクトへのアクセス特権を持つシステム内のオブジェクトのグループを識別するグループ識別子をターゲット・オブジェクトと共に記憶するステップと、
第２のサーバ・オブジェクトの制御下で、
コンテナ・オブジェクトを入手するステップと、
第２のサーバ・オブジェクトがその代理として動作する本人を識別する本人識別子を含む要求を第１のサーバ・オブジェクトに送ってターゲット・オブジェクトへのアクセスを要求するステップと、
第１のサーバの制御下で、
ターゲット・オブジェクトに記憶されているグループ識別子と第２のサーバからの要求に含まれている本人識別子とを使用して、第２のサーバがターゲット・オブジェクトにアクセスする許可を有することを検証するステップとを含む方法。

【請求項３】　コンテナ・オブジェクトを入手するステップが、
第１のサーバ・オブジェクトの制御下で、
コンピュータ・システム内のターゲット・オブジェクトの場所を示すターゲット・オブジェクト・リファレンスをクライアント・オブジェクトに送るステップと、
クライアント・オブジェクトの制御下で、
クライアント・オブジェクトが属するグループのメンバーの代理として動作する第２のサーバを見つけるステップと、
クライアント・オブジェクトから第２のサーバ・オブジェクトへの要求がターゲット・オブジェクト・リファレンスを含み、クライアント・オブジェクトが属するグループを識別するグループ識別子も含む要求を見つけた第２のサーバに送って、第２のサーバがターゲット・オブジェクトを参照するコンテナ・オブジェクトを入手するように要求するステップと、
第２のサーバの制御下で、
コンテナ・オブジェクトを入手するステップと、
コンテナ・オブジェクトにターゲット・オブジェクト・リファレンスとグループ識別子を記憶するステップとをさらに含む請求項２に記載の方法。

【請求項４】　第２のサーバから第１のサーバに要求を送るステップが、
クライアント・オブジェクトの制御下で、
コンテナ・オブジェクトを使用するために、コンテナ・オブジェクトのリファレンスとクライアント・オブジェクトの本人の識別子とを含む要求を第２のサーバに送るステップと、
第２のサーバの制御下で、
クライアント・オブジェクトからの要求に応答して、ターゲット・オブジェクトにアクセスするために、ターゲット・オブジェクトのリファレンスと第２のサーバがその代理として動作する本人の識別子とを含む要求を第１のサーバに送るステップとをさらに含む請求項２に記載の方法。

【請求項５】　第１のサーバの制御下で、
第２のサーバから第１のサーバに送られた本人の識別子を使用して第２のサーバを認証するステップをさらに含む請求項４に記載の方法。

【請求項６】　第２のサーバが認証され、ターゲット・オブジェクトへのアクセス権を有するグループのメンバーであると判断された場合、
第１のサーバのリファレンスから偽造不能な番号を取り出して、

取り出した偽造不能番号をターゲット・オブジェクトと共に記憶されている偽造不能番号と比較することによって、
第２のサーバがターゲット・オブジェクトに要求された方法でアクセスすることを許可されているか否かを判断するステップと、
偽造不能番号が一致する場合、第２のサーバのアクセス権にしたがって第２のサーバがターゲット・オブジェクトにアクセスすることを許可するステップとをさらに含むことを特徴とする、請求項５に記載の方法。
【請求項７】　第２のサーバがターゲット・オブジェクトにアクセスする許可を有していることを検証するステップが、
第１のサーバの制御下で、
ターゲット・オブジェクトからグループ識別子を取り出すステップと、
取り出したグループ識別子と本人識別子を、本人がターゲット・オブジェクトへのアクセス権を有するグループのメンバーであるか否かを判断する要求と共にメンバーシップ機構に送るステップと、
第２のサーバがターゲット・オブジェクトへのアクセス権を有するグループのメンバーである本人の代理として動作すると判断された場合に第２のサーバがターゲット・オブジェクトにアクセスすることを許可するステップとをさらに含む請求項２に記載の方法。
【請求項８】　クライアント・オブジェクトから第１のサーバ・オブジェクトに、第１のサーバ・オブジェクトがターゲット・オブジェクトを作成するように指示する要求を送るステップと、
第１のサーバ・オブジェクトの制御下で、
ターゲット・オブジェクトを作成するステップと、
グループ・メンバーがターゲット・オブジェクトに関して有するアクセス権の標識を記憶するステップとをさらに含む請求項２に記載の方法。
【請求項９】　分散コンピュータ・システムが、クライアント・オブジェクトと、第１のサーバ・オブジェクトと、ターゲット・オブジェクトと、第２のサーバ・オブジェクトとを含み、各オブジェクトがコンピュータ・システムにあるオブジェクトの１つまたは複数の指定されたグループに属する場合に、分散コンピュータ・システム内のシステム資源へのアクセス制御を容易にするコンピュータ・システムであって、
ターゲット・オブジェクトへのアクセス特権を有するシステム内のオブジェクトのグループを識別するグループ識別子をターゲット・オブジェクトと共に記憶するように構成された第１のサーバ・オブジェクトと、
コンテナ・オブジェクトを入手し、要求が第２のサーバ・オブジェクトがその代理として動作する本人を識別する本人識別子を含むターゲット・オブジェクトへのアクセスを要求する要求を第１のサーバ・オブジェクトに送るように構成された第２のサーバ・オブジェクトと、
ターゲット・オブジェクトに記憶されたグループ識別子と第２のサーバからの要求に含まれた本人識別子とを使用して、第２のサーバがターゲット・オブジェクトにアクセスする許可を有することを検証するように構成された第１のサーバとを含むシステム。
【請求項１０】　コンテナ・オブジェクトの入手の構成が、
第１のサーバオブジェクトが、
コンピュータ・システム内のターゲット・オブジェクトの場所を示すターゲット・オブジェクト・リファレンスをクライアント・オブジェクトに送るように構成され、
クライアント・オブジェクトが、
クライアント・オブジェクトが属するいくつかのグループの代理として動作する第２のサーバを見つけ、
クライアント・オブジェクトから第２のサーバ・オブジェクトへの要求がターゲット・オブジェクト・リファレンスを含み、クライアント・オブジェクトが属するグループを識別するグループ識別子も含む要求を見つけた第２のサーバに送って、第２のサーバがターゲット・オブジェクトを参照するコンテナ・オブジェクトを入手するように要求するように構成され、
第２のサーバが、
コンテナ・オブジェクトを入手し、
コンテナ・オブジェクトにターゲット・オブジェクト・リファレンスとグループ識別子を記憶するように構成されているシステムをさらに含む請求項９に記載のシステム。
【請求項１１】　第２のサーバから第１のサーバに要求を送る構成が、
クライアント・オブジェクトが、
コンテナ・オブジェクトを使用するために、コンテナ・オブジェクトのリファレンスとクライアント・オブジェクトの本人の識別子とを含む要求を第２のサーバに送るように構成され、
第２のサーバが、
クライアント・オブジェクトからの要求に応答して、ターゲット・オブジェクトにアクセスするために、ターゲット・オブジェクトのリファレンスと第２のサーバがその代理として動作する本人の識別子とを含む要求を第１のサーバに送るように構成されているシステムをさらに含む請求項９に記載の方法。
【請求項１２】　第２のサーバから第１のサーバに送られた本人の識別子を使用して第２のサーバを認証するように構成された第１のサーバをさらに含む請求項１１に記載のシステム。
【請求項１３】　第２のサーバが認証され、ターゲット・オブジェクトへのアクセス権を有するグループのメンバーであると判断された場合、
第１のサーバのリファレンスから偽造不能な番号を取り

出して、
取り出した偽造不能番号をターゲット・オブジェクトと共に記憶されている偽造不能番号と比較することによって、
第２のサーバがターゲット・オブジェクトに要求された方法でアクセスすることを許可されているか否かを判断し、
偽造不能番号が一致する場合、第２のサーバのアクセス権にしたがって、第２のサーバがターゲット・オブジェクトにアクセスするように構成された機構をさらに含む請求項１２に記載のシステム。
【請求項１４】　第２のサーバがターゲット・オブジェクトにアクセスする許可を有していることを検証する構成が、
第１のサーバが、
ターゲット・オブジェクトからグループ識別子を取り出し、
取り出したグループ識別子と本人識別子を、本人がターゲット・オブジェクトへのアクセス権を有するグループのメンバーであるか否かを判断する要求と共にメンバーシップ機構に送り、
第２のサーバがターゲット・オブジェクトへのアクセス権を有するグループのメンバーである本人の代理として動作すると判断された場合に第２のサーバがターゲット・オブジェクトにアクセスすることを許可するように構成されているシステムをさらに含む請求項９に記載の方法。
【請求項１５】　クライアント・オブジェクトから第１のサーバ・オブジェクトに、第１のサーバ・オブジェクトがターゲット・オブジェクトを作成するように指示する要求を送るように構成された機構をさらに含み、
第１のサーバ・オブジェクトが、
ターゲット・オブジェクトを作成し、
グループ・メンバーがターゲット・オブジェクトに関して有するアクセス権の標識を記憶するように構成されている請求項９に記載の方法。
【請求項１６】　分散コンピュータ・システムが、クライアント・オブジェクトと、第１のサーバ・オブジェクトと、ターゲット・オブジェクトと、第２のサーバ・オブジェクトとを含み、各オブジェクトがコンピュータ・システムにあるオブジェクトの１つまたは複数の指定されたグループに属する場合に、分散コンピュータ・システム内のシステム資源へのアクセス制御を容易にするコンピュータ・プログラムであって、
ターゲット・オブジェクトへのアクセス特権を有するシステム内のオブジェクトのグループを識別するグループ識別子をターゲット・オブジェクトと共に記憶するように構成された、第１のサーバ・オブジェクトのためのコードと、
コンテナ・オブジェクトを入手し、要求が第２のサーバ・オブジェクトがその代理として動作する本人を識別する本人識別子を含むターゲット・オブジェクトへのアクセスを要求する要求を第１のサーバ・オブジェクトに送るように構成された、第２のサーバ・オブジェクトのためのコードと、
ターゲット・オブジェクトに記憶されたグループ識別子と第２のサーバからの要求に含まれた本識別子とを使用して、第２のサーバがターゲット・オブジェクトにアクセスする許可を有することを検証するように構成された、第１のサーバのためのコードとを含み、
前記各コードが有形の媒体に記憶されていることを特徴とするプログラム。
【請求項１７】　コンテナ・オブジェクトを入手するコードが、
コンピュータ・システム内のターゲット・オブジェクトの場所を示すターゲット・オブジェクト・リファレンスをクライアント・オブジェクトに送るように構成された、第１のサーバ・オブジェクトのためのコードと、、
クライアント・オブジェクトが属するいくつかのグループの代理として動作する第２のサーバを見つけ、
クライアント・オブジェクトから第２のサーバ・オブジェクトへの要求がターゲット・オブジェクト・リファレンスを含み、クライアント・オブジェクトが属するグループを識別するグループ識別子も含む要求を見つけた第２のサーバに送って、第２のサーバがターゲット・オブジェクトを参照するコンテナ・オブジェクトを入手するように要求するように構成された、クライアント・オブジェクトのためのコードと、
コンテナ・オブジェクトを入手し、コンテナ・オブジェクトにターゲット・オブジェクト・リファレンスとグループ識別子を記憶するように構成された、第２のサーバのためのコードとをさらに含む請求項１６に記載のプログラム。
【請求項１８】　第２のサーバから第１のサーバに要求を送るコードが、
コンテナ・オブジェクトを使用するために、コンテナ・オブジェクトのリファレンスとクライアント・オブジェクトの本人の識別子とを含む要求を第２のサーバに送るように構成された、クライアント・オブジェクトのためのコードと、
クライアント・オブジェクトからの要求に応答して、ターゲット・オブジェクトにアクセスするために、ターゲット・オブジェクトのリファレンスと第２のサーバがその代理として動作する本人の識別子とを含む要求を第１のサーバに送るように構成された、第２のサーバのためのコードとをさらに含む請求項１６に記載のプログラム。
【請求項１９】　第２のサーバから第１のサーバに送られた本人の識別子を使用して第２のサーバを認証するように構成された、第１のサーバのためのコードをさらに

含む請求項１８に記載のプログラム。
【請求項２０】　第２のサーバが認証され、ターゲット・オブジェクトへのアクセス権を有するグループのメンバーであると判断された場合、
第１のサーバのリファレンスから偽造不能な番号を取り出して、
取り出した偽造不能番号をターゲット・オブジェクトと共に記憶されている偽造不能番号と比較することによって、
第２のサーバがターゲット・オブジェクトに要求された方法でアクセスすることを許可されているか否かを判断し、
偽造不能番号が一致する場合、第２のサーバのアクセス権を条件として、第２のサーバがターゲット・オブジェクトにアクセスするように構成されたコードをさらに含む請求項１９に記載のプログラム。
【請求項２１】　第２のサーバがターゲット・オブジェクトにアクセスする許可を有していることを検証するコードが、
ターゲット・オブジェクトからグループ識別子を取り出し、
取り出したグループ識別子と本人識別子を、本人がターゲット・オブジェクトへのアクセス権を有するグループのメンバーであるか否かを判断する要求と共にメンバーシップ機構に送り、
第２のサーバがターゲット・オブジェクトへのアクセス権を有するグループのメンバーである本人の代理として動作すると判断された場合に第２のサーバがターゲット・オブジェクトにアクセスすることを許可するように構成された、第１のサーバのためのコードをさらに含む請求項１６に記載のプログラム。
【請求項２２】　クライアント・オブジェクトから第１のサーバ・オブジェクトに、第１のサーバ・オブジェクトがターゲット・オブジェクトを作成するように指示する要求を送るように構成されたコードをさらに含み、
第１のサーバ・オブジェクトのためのコードが、
ターゲット・オブジェクトを作成し、
グループ・メンバーがターゲット・オブジェクトに関して有するアクセス権の標識を記憶するように構成されている請求項１６に記載のプログラム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明の方法およびシステムは、一般にはコンピュータ・システムにおけるセキュリティを与えることに関し、より特定的には、オブジェクト・リファレンスまたはケーパビリティに結びつけられたグループ識別標識を使用してシステム資源へのアクセスを制御することに係わる。
【０００２】
【従来の技術】オブジェクト指向システムにおいて、オブジェクトとは、データとデータを取り扱うために呼び出すことができる操作を含む構成要素である。操作（「メソッド」とも呼ぶ）は、オブジェクトに呼を送ることによって、オブジェクト上に呼び出される。各オブジェクトは、そのタイプのオブジェクトに対して実行することができる操作を定義するオブジェクト・タイプを有する。１つのオブジェクト・タイプは、他のオブジェクト・タイプのために定義され、実施されたオブジェクト操作を継承することができる。オブジェクト指向設計およびプログラミング技法の詳細については、参照により本明細書に組み込まれるＢｅｒｔｒａｎｄＭｅｙｅｒによる「Ｏｂｊｅｃｔ－Ｏｒｉｅｎｔｅｄ　Ｓｏｆｔｗａｒｅ　Ｃｏｎｓｔｒｕｃｔｉｏｎ」（Ｐｒｅｎｔｉｃｅ－Ｈａｌｌ　１９８８）を参照されたい。
【０００３】クライアント－サーバ・コンピューティングでは、一般に、コンピュータを接続するネットワークを介して互いに通信することができる１組のコンピュータが存在する。これらのコンピュータのいくつかは、他のコンピュータに対するサービスまたは機能の提供側の役割を果たす。このサービスまたは機能の提供側は「サーバ」と呼ばれ、サービスまたは機能の消費側は「クライアント」と呼ばれる。このクライアント－サーバ・モデルは、同じコンピュータ上で別個のプログラムまたはプロセスが実行され、それらが何らかの保護された機構を介して互いに通信し、機能の提供側と消費側として機能している場合にも一般化される。
【０００４】クライアントサーバ・モデルに基づくオブジェクト指向分散システムには、クライアントにオブジェクト指向インタフェースを提供するサーバが存在する。これらのサーバは、データと、当該タイプのオブジェクトにより許可された操作に従ってデータを取り扱うそのデータに関連するソフトウェアとから成るオブジェクトをサポートする。クライアントは、サーバに呼を送信することによって、これらのオブジェクトへのアクセスを獲得することができ、それらのオブジェクトに対して呼を実行することができる。サーバでは、そのオブジェクトに関連するソフトウェアを介してこれらの呼が実行される。次に、それらの呼の結果がクライアントに送り戻される。
【０００５】現在、いくつかの会社が、このようなオブジェクトを互いに共用することができるようにする特定のオブジェクト定義およびインタフェースの標準化に合意している。このようなオブジェクトの会社間共用への参加を可能にするように設計された１つのシステムを、「分散オブジェクト環境（「ＤＯＥ」）」と呼び、サン・マイクロシステムズ・インコーポレイテッド（サン、ＤＯＥ、およびサン・マイクロシステムズ・インコーポレイテッドは、米国およびその他の国でのサン・マイクロシステムズ・インコーポレイテッドの商標または登録商標である。）が作成した。

【０００６】ＤＯＥはオブジェクト指向システムであり、クライアントからＤＯＥオブジェクトへの遠隔アクセスを提供する。サーバ・アプリケーションがＤＯＥオブジェクトを実現する。所与のＤＯＥオブジェクトについて、ＤＯＥサーバはＤＯＥオブジェクトを指すポインタとして機能する「オブジェクト・リファレンス」を作成することができる。ＤＯＥオブジェクト・リファレンスは、１つの機械上または異なる機械間の異なるプロセス間で次々に渡すことができ、その場合でも元のオブジェクトを指すことになる。

【０００７】１つの場所のクライアント・アプリケーションがＤＯＥオブジェクト・リファレンスを獲得すると、そのアプリケーションはターゲットＤＯＥオブジェクトに呼出し（メソッド呼出し要求）を送ることができる。次に、ターゲットＤＯＥオブジェクトは、場合によってはその内部状態（そのデータ）を更新し、場合によっては何らかの結果をその呼出し側に戻すことによって、それらの呼出しを実行することができる。メソッド呼出しを処理する一環として、サーバはそれ自体が他のオブジェクトを呼び出すことができ、オブジェクト呼出しの連鎖が形成される。

【０００８】ユーザの直接制御外にある実体とのこのようなオブジェクト共用の登場により、いくつかのセキュリティ問題が生ずる。たとえば、ＤＯＥユーザが、多くの組の機械に分散しているオブジェクトにアクセスすることができるようにすることが望ましい。しかし、許可されたユーザだけがオブジェクトをアクセスすることができるようにして、オブジェクトがカプセル化するデータを無許可のユーザが使用したり変更したりすることができないようにすることが不可欠である。

【０００９】このようなセキュリティ問題の部分的な解決策として、いくつかのサーバは、そのサーバのオブジェクトへのセキュリティ保護されたアクセスを設け、適正に指定されたユーザだけがオブジェクトにアクセスすることができるようにする。クライアント・アプリケーションがセキュリティ保護されたオブジェクトにアクセスしたい場合は、そのセキュリティ保護されたオブジェクトの遂行を含むサーバとの「認証済み接続」を確立しなければならない。この接続を確立すると同時に、クライアント・アプリケーションは、クライアント・アプリケーションがどのユーザを表しているかをサーバに示さなければならない。したがって、たとえばクライアント・アプリケーションは人間のユーザであるスーザンを表している場合がある。クライアント・コンピュータのログイン業務の一部として、スーザンと称する人間のユーザは、恐らくある種の認証情報、たとえばパスワードを、クライアント・コンピュータに与えなければならない。認証済み接続が確立された後、サーバはその接続が所与のユーザを表す権限を与えられているアプリケーションへの接続であることを認める。サーバはそのユーザの名前を記録し、そのユーザの名前をその接続と関連づける。認証済み接続を確立する技術は、よく理解されている。たとえば、Ｂｕｔｌｅｒ Ｌａｍｐｓｏｎ、Ｍａｒｔｉｎ Ａｂａｄｉ、Ｍｉｃｈａｅｌ Ｂｕｒｒｏｗｓ、およびＥｄｗａｒｄ Ｗｏｂｂｅｒによる「Ａｕｔｈｅｎｔｉｃａｔｉｏｎ ｉｎ Ｄｉｓｔｒｉｂｕｔｅｄ Ｓｙｓｔｅｍｓ：Ｔｈｅｏｒｙ ａｎｄ Ｐｒａｃｔｉｖｅ」（ＡＣＭ Ｔｒａｎｓａｃｔｉｏｎｓ ｏｎ Ｃｏｍｐｕｔｅｒ Ｓｙｓｔｅｍｓ，１０（４），Ｎｏｖｅｍｂｅｒ １９９２）を参照されたい。

【００１０】通常のＤＯＥモデルは、クライアントが遠隔オブジェクトに対する操作を呼び出すものである。サーバは、要求が認証済み接続で発行されるように要求することができ、したがってクライアント・アプリケーションが認証済みユーザを表していることを検証することができる。サーバは次にその認証済みユーザが、その操作を行うことを本当に許可されているか調べることができる。

【００１１】ユーザがサーバに、そのサーバが他のセキュリティ保護されたサーバにアクセスする必要がある何らかのアクションを行わせようとすると直ちに複雑な問題が生ずる。たとえば、ユーザはクライアント・アプリケーションに複合文書（たとえばスプレッド・シート・グラフと説明テキストが含まれた年間売上げ報告）を入手するように要求し、その一部が第１のサーバにあり（たとえばテキスト）、一部が第２のサーバにある（たとえばグラフ）場合がある。第１のサーバは、要求ユーザを認証し、ユーザがその要求を行うことを許可されていることを検証することができる。しかし、次に第１のサーバが、ユーザ応答を完了させるために何らかのデータを求めて第２のサーバにアクセスしなければならない場合、第２のサーバは、第１のサーバを認証しなければならず、第１のサーバがクライアントによるアクセスを認められたか、またはオブジェクトに対して要求されたアクションを実行する適切なアクセス許可を有していることを確認しなければならない。この問題を委託問題と呼ぶ。これは、クライアントのジョブを行わせることができるようにするためにクライアントがその権限をサーバに委託する必要があるときに発生する。

【００１２】

【発明が解決しようとする課題】ユーザが第２のサーバにアクセスする際に第１のサーバに対してユーザの名前で代行するように委託するには、ユーザは多くの機械を信任する必要があり、ユーザはセキュリティ攻撃にさらされる。あるいは、ユーザは小規模な１組の既知の機械だけを信任しなければならず、所望のオブジェクトに対するユーザのアクセスが著しく制限される。同様に、ネットワーク全体に分散したクライアントからのアクセス要求を受け入れることは、サーバ自体にとってかなりのセキュリティ・リスクとなる。したがって、分散ネット

ワーク環境においてアクセス制御権を安全に委託する改良された方法およびシステムを開発することが望ましいであろう。

【００１３】本発明は、ネットワーク環境内の分散コンピュータ・システムにおける様々なサーバからのアクセス要求の安全な取扱いという問題を解決する精巧で簡素な方法を提供することを課題とする。

【００１４】

【課題を解決するための手段】本発明は、分散コンピュータ・システムにおける資源へのアクセスを安全に制御する改良された方法とシステムを提供する。本発明の一実施態様は、グループ標識を記憶してターゲット・オブジェクトに結びつけ、次にメンバーシップ検査を使用して、ターゲット・オブジェクトへのアクセスを要求するクライアント・オブジェクトが、そのグループのメンバーであるユーザの代理として動作するかどうかを判断する。このようにして、本発明は要求側オブジェクトのアクセス権を検証するために、一部の従来技術のシステムで一般的に行われていたコストのかかる暗号操作を行わなくても済むようにする。

【００１５】本発明の第２の実施態様は、グループ識別標識を記憶してターゲット・オブジェクト・リファレンスに結びつけ、次にそのターゲット・オブジェクト・リファレンスをシステム内のクライアント・オブジェクトに渡す。ターゲット・オブジェクト・リファレンスはグループ識別標識項目を含むため、第１のクライアント・オブジェクトはシステム内の他のどのクライアントが識別されているグループのメンバーであるかを判断することができる。この判断によって、第１のクライアント・オブジェクトは、まずターゲット・オブジェクトのためにサーバと通信しなくても、そのターゲット・オブジェクト・リファレンスをグループの他のメンバーに渡すことができる。このようにして、本発明はターゲット・オブジェクトのためにサーバと通信するコストのかかるトランザクション・コストを省く。

【００１６】

【発明の実施の形態】

表記および用語

以下の詳細な説明は、主としてコンピュータ・システム内のデータ・ビットに対する操作の方法と記号表現によって示す。これらの方法の説明と表現は、データ処理技術業者がその作業を他の当業者に最も効果的に伝えるために使用する手段である。

【００１７】本明細書において、また一般的に、方法とは所望の結果に至る自己矛盾のない一連のステップであると考えられる。これらのステップは、物理数量の物理的操作を必要とする。これらの数量は、記憶、転送、結合、比較、またはその他の操作が可能な電気信号または磁気信号の形態をとるのが普通であるが、必ずしもそうであるとは限らない。主として一般的使用の理由から、これらの信号を時にはビット、値、要素、記号、文字、項、数字、または同様のものと呼ぶと好都合であることがわかる。しかし、これらの用語および同様の用語はすべて、適切な物理数量と関連づけられるべきものであり、それらの物理数量に適用された便利な符号に過ぎないことを銘記されたい。

【００１８】本発明の操作を実行するのに有用な機械には、汎用ディジタル・コンピュータまたは同様の装置が含まれる。汎用コンピュータは、コンピュータに記憶されたコンピュータ・プログラムによって選択的に起動または再構成することができる。専用コンピュータも、本発明の操作を実行するために使用することができる。要するに、本明細書で説明し、示唆する方法の使用は、特定のコンピュータ構成には限定されない。

【００１９】好ましい方法の概要

本発明の実施形態は、分散コンピュータ・システムにおける資源へのアクセスを安全に制御する改良された方法およびシステムを提供する。本発明の一実施形態は、グループ標識を記憶してターゲット・オブジェクトに結びつけ、次にメンバーシップ検査を使用して、ターゲット・オブジェクトへのアクセスを要求するクライアント・オブジェクトが、そのグループのメンバーであるユーザの代理として動作するかどうかを判断する。このようにして、本発明は要求側オブジェクトのアクセス権を検証するために、一部の従来技術のシステムで一般的に行われていたコストのかかる暗号操作を行わなくても済むようにする。

【００２０】本発明の第２の実施形態は、グループ識別標識を記憶してターゲット・オブジェクト・リファレンスに結びつけ、次にそのターゲット・オブジェクト・リファレンスをシステム内のクライアント・オブジェクトに渡す。ターゲット・オブジェクト・リファレンスはグループ識別標識項目を含むため、第１のクライアント・オブジェクトはシステム内の他のどのクライアントが識別されているグループのメンバーであるかを判断することができる。この判断によって、第１のクライアント・オブジェクトは、ターゲット・オブジェクトのためにまずサーバと通信しなくても、そのターゲット・オブジェクト・リファレンスをグループの他のメンバーに渡すことができる。このようにして、本発明はターゲット・オブジェクトのためにサーバと通信する高価なトランザクション・コストを省く。

【００２１】好ましいシステムの概要

図１は、本発明の好ましい実施形態を実施するためのコンピュータ・システム１００のブロック図である。コンピュータ・システム１００は、コンピュータ１０１と、入力装置１０３と、記憶装置１０５と、表示装置１０７とを含む。表示装置１０７はグラフィカル・ユーザ・インタフェース（ＧＵＩ）１０９を表示する。ＧＵＩはアイコンによって情報を提示し、ユーザはアイコンを指し

示すかまたは操作することによってコマンドを呼び出す。コンピュータ１０１は、プロセッサ１１１と、メモリ１１３と、プロセッサ１１１と入力装置１０３や表示装置１０７などの周辺装置との間のコミュニケーションを可能にするインタフェース１１５とを備える。

【００２２】コンピュータ・メモリは、クライアント・オブジェクト１１７と、複合文書サーバ・オブジェクト１１９と、スプレッドシート・サーバ・オブジェクト１２１とを含むいくつかの項目を保持する。メモリ１１３の内容については以下で詳述する。

【００２３】本発明の実施形態

本発明の実施形態については例を使用して説明するのが恐らく最もわかりやすいであろう。本明細書で説明する２つの実施形態について、複合文書の作成と印刷に焦点を合わせて説明する。もちろん、ほかの用途にも使用できるのはいうまでもない。

【００２４】複合文書は典型的にはテキストとグラフィックの両方を含む。たとえば、年次売上げ増加率を図示するチャートおよびグラフと説明テキストを含む年間売上げ報告書は、複合文書として実現される。チャートおよびグラフは、スプレッドシート・サーバの制御下に記憶され、複合文書のテキストは複合文書サーバの制御下にチャートおよびグラフとのリンクと共に記憶されることが多い。

【００２５】これらの例は、１つのコンピュータ上にある様々なプロセス間で行われるが、当業者なら本明細書の教示がネットワーク環境全体に分散されたオブジェクトおよびプロセスにも等しく適用可能であることを理解するであろう。

【００２６】しかし、いずれの例でも処理を開始する前に、コンピュータ・システム１００内に特定の前提条件が存在する。ユーザ（または「本人」）がシステム１００へのログオンに成功し、信用証明を獲得し、クライアント・オブジェクト１１７を呼び出していることが前提となる。本例では、クライアント・オブジェクト１１７は典型的には、ワードプロセッシング・アプリケーションを含むプロセスに対応する。次に、そのオブジェクト１１７が本人の代理の役割を果たすことを示すために、本人信用証明がクライアント・オブジェクト１１７と共に記憶される。さらに、本人はコンピュータ・システム１００上でアクセス特権を有する他の本人のグループに関連づけられる。たとえば、営業担当者は営業部のグループに関連づけられる。システム１００内に定義されている各グループは、そのグループに関連づけられた固有のグループ識別子を有する。さらに、本人の代理を果たすオブジェクトが、指定されたグループのメンバーであるか否かを判断するために、メンバーシップ信用証明を検査する機構（たとえば機構１２３）がなければならない。システム１００のこの態様を実施するために、メンバーシップ機構を実施する任意の周知の方法またはシステムを使用することができる。

【００２７】第１の実施形態

図２は、システム資源へのアクセスを安全に制御する第１の実施形態の好ましいステップを示す流れ図である。図２のステップは、典型的にはユーザ入力に応答して開始される。本人が、スプレッドシートを作成する要求をクライアント１１７で開始するとする（ステップ２０１）。この入力に応答して、クライアント・オブジェクト１１７はスプレッドシート・サーバ・オブジェクトに「作成」要求を送信する（ステップ２０３）。この要求は、スプレッドシート・オブジェクトをインスタンス化することを指示する。この要求には、複合文書サーバが代理として動作するユーザに関連づけられたグループ識別子も含まれる。

【００２８】スプレッドシート・サーバ・オブジェクトは要求を受け取ってスプレッドシート・オブジェクトを作成する（ステップ２０５）。次に、スプレッドシート・サーバ・オブジェクトは、スプレッドシート・オブジェクトをグループ識別子付きで、グループ・メンバーがそのスプレッドシート・オブジェクトに関して有するアクセス権の標識と共に記憶する（ステップ２０７）。最後に、スプレッドシート・サーバ・オブジェクトは、偽造不能な番号を生成し、その偽造不能番号をスプレッドシート・オブジェクトと共に記憶する（ステップ２０９）。このようにして、スプレッドシート・サーバ・オブジェクトは、サーバ・オブジェクトへのアクセスを要求するクライアント・オブジェクトによってその偽造不能番号と共に提示されると、要求側クライアントがそのスプレッドシート・オブジェクトにアクセスする権限を有するというある種の確証を持つことができる。この偽造不能番号はしばしば「ケーパビリティ」呼ばれる。偽造不能番号は、計算的に判断するのが困難な番号である。

【００２９】スプレッドシート・サーバ・オブジェクトは次に、クライアント・オブジェクト１１７にスプレッドシート・オブジェクト・リファレンスを送る（ステップ２１１）。好ましい実施形態では、スプレッドシート・オブジェクト・リファレンスは、直前に生成された偽造不能番号を含む。

【００３０】スプレッドシート・サーバ・オブジェクトがクライアント・オブジェクトに処理制御を返すと、グループ内の本人の代理として動作するクライアント・オブジェクトは複合文書サーバを見つけ出す（ステップ２１３）。次に、クライアント・オブジェクトは複合文書を作成する要求を複合文書サーバ１１９に送る（ステップ２１５）。「作成」要求には、複合文書を作成するという指示が含まれる。「作成」要求には、複合文書サーバがその複合文書にどのスプレッドシート・オブジェクトを組み込むべきかわかるように、スプレッドシート・オブジェクト・リファレンスも含まれる。最後に「作

成」要求には、複合文書へのアクセスを要求する本人がその複合文書へのアクセスを許可されているかどうかを、複合文書サーバが後で判断することができるように、選択されたグループ識別子が含まれる。

【００３１】複合文書サーバは、複合文書を作成し、その複合文書にスプレッドシート・オブジェクト・リファレンスとグループ識別子を格納する（ステップ２１７）。次に、複合文書サーバは、偽造不能番号を生成し、その偽造不能番号を複合文書オブジェクトと共に記憶する。このようにして、複合文書サーバ・オブジェクトは、その複合文書オブジェクトへのアクセスを要求するクライアント・オブジェクトによってその偽造不能番号が提示されると、要求側クライアントがその複合文書オブジェクトにアクセスする権限を有するというある種の確証を持つことができる。

【００３２】複合文書サーバ・オブジェクト１１９は次に、クライアント・オブジェクト１１７に複合文書オブジェクト・リファレンスを送る（ステップ２１９）。好ましい実施形態では、複合文書オブジェクト・リファレンスは、複合文書サーバ・オブジェクトによって生成された偽造不能番号を含む。

【００３３】その後のある時点で、クライアント・オブジェクトは複合文書サーバに印刷要求を送る（ステップ２２１）。「印刷」要求によって、複合文書リファレンスとクライアントの本人の識別標識が複合文書サーバに渡される。クライアントは、任意の周知の認証機構を使用して、クライアントの本人の代理として動作する権利を有することを複合文書サーバに対して証明する。複合文書リファレンスとクライアントの本人の識別標識を複合文書サーバに渡すことによって、複合文書サーバはどの複合文書を印刷すべきかを判断することができ、認証された識別標識がその複合文書が作成されたときに指定されたグループに属することを検査し、オブジェクト・リファレンス内の偽造不能番号をオブジェクト内の偽造不能番号と比較することによって、クライアント・オブジェクト１１７がその複合文書を印刷する許可を持っていることを検証することができる。

【００３４】複合文書を印刷するために、複合文書サーバはスプレッドシート・オブジェクトに関連づけられたデータを持っている必要がある。したがって、複合文書サーバはスプレッドシート・サーバに「データ入手」要求を送る（ステップ２２３）。「データ入手」要求にはスプレッドシート・オブジェクト・リファレンスが含まれ、どのスプレッドシート・オブジェクトからデータを取り出すべきかがスプレッドシート・サーバにわかるようになっている。「データ入手」要求には複合文書サーバが代理として動作する本人の識別表記をも含む。

【００３５】複合文書サーバはそれ自体の正当性をスプレッドシート・サーバに対して証明する（ステップ２２５）。出願人の実施形態のこの態様を実施するために、本人を認証する任意の周知の技法を使用することができる。複合文書サーバの認証が成功すると、スプレッドシート・サーバは複合文書サーバが、スプレッドシート・オブジェクトからデータを取り出すことを許可するアクセス権を持っているかどうかを判断しようとする。アクセス権を判断するためにスプレッドシート・サーバは、スプレッドシート・オブジェクトからグループ識別子を検索する。次にスプレッドシート・サーバは、グループ識別子と認証された本人識別子を、スプレッドシート・オブジェクトへのアクセス権を持つグループのメンバーであるかどうかを判断するよう求める要求と共に、メンバーシップ機構１２３に送る（ステップ２２７）。出願人の実施形態のこの態様を実施するためには、グループ・メンバーシップを検査する任意の周知の機構を使用することができる。

【００３６】複合文書サーバの認証済み本人が指定されたグループのメンバーである場合、スプレッドシート・サーバは、複合文書がスプレッドシート・オブジェクトにアクセスすることを許可されていることを確認するために、さらに他の検査を行う。スプレッドシート・サーバはスプレッドシート・サーバ・リファレンスから偽造不能番号を取り出し、それをスプレッドシート・サーバ・オブジェクトと共に記憶されている偽造不能番号と比較する（好ましい実施形態では、このステップを先に実施することが好ましい）（ステップ２２９）。偽造不能番号が一致する場合、スプレッドシート・サーバはオブジェクトと共に記憶されているアクセス権を条件として、複合文書サーバがスプレッドシート・オブジェクトから必要なデータを取り出すのを許可する（ステップ２３１）。

【００３７】スプレッドシート・データが取り出されると、複合文書サーバは印刷のためにその複合文書データを印刷サーバに送る（ステップ２３３）。

【００３８】この第１の実施形態に付随する利点の１つは、オブジェクトへのアクセスを要求するクライアントがそのオブジェクトへのアクセスを許可されているかどうかを判断するために暗号操作が不要である点である。暗号操作ではなく、第１の実施形態はスプレッドシート・オブジェクトの状態データ内でグループ識別子を維持し、そのグループ識別子を使用して、要求側クライアントが適切なグループのメンバーであるユーザの代理として動作するか否かを判断することによって、この許可検査を行う。このグループ・メンバーシップ検査は典型的には、暗号操作を行うよりもコストがかからない。

【００３９】第１の実施形態のもう一つの利点は、スプレッドシート・オブジェクトで維持されている状態データを使用するだけで、誰がオブジェクトへのアクセス権を持っているかをスプレッドシート・サーバが判断することができることである。他の従来技術では、オブジェクト・リファレンスのみがアクセス権情報を格納してい

たため、これは不可能だった。アクセス権情報がオブジェクト自体とともに格納されていなかった。

【００４０】第２の実施形態

図３は、システム資源へのアクセスを安全に制御する第２の実施形態の好ましいステップを示す流れ図である。図３のステップは、典型的にはユーザ入力に応答して開始される。本人がスプレッドシートを作成する要求をクライアント１１７で開始するとする（ステップ３０１）。この入力に応答して、クライアント・オブジェクト１１７がスプレッドシート・サーバ・オブジェクトに「作成」要求を送る（ステップ３０３）。この要求は、スプレッドシート・オブジェクトをインスタンス化することを指示する。この要求には、複合文書サーバが代理として動作する本人に関連づけられたグループ識別子も含まれる。

【００４１】スプレッドシート・サーバ・オブジェクトは要求を受け取ってスプレッドシート・オブジェクトを作成する（ステップ３０５）。次にスプレッドシート・サーバ・オブジェクトは、クライアント・オブジェクト１１７にスプレッドシート・オブジェクト・リファレンスを送る（ステップ３０７）。第２の実施形態では、スプレッドシート・オブジェクト・リファレンスは「作成」要求と共に送られたグループ識別子と、そのグループのアクセス権特権を示す項目と、スプレッドシート・オブジェクト識別子とを含む。スプレッドシート・オブジェクト・リファレンスは、暗号一方向ハッシュ関数を使用してオブジェクト・リファレンス・データについて暗号チェックサムを出す。暗号チェックサムは、スプレッドシート・オブジェクト・リファレンス内に、またはそれと付随させて保管もされる。そうすると、スプレッドシート・オブジェクト・リファレンスは偽造に対する保護が強化される。

【００４２】スプレッドシート・オブジェクト・サーバがクライアント・オブジェクトに処理制御を返すと、クライアント・オブジェクトは複合文書を作成する要求を複合文書サーバ１１９に送る（ステップ３０９）。「作成」要求には、複合文書を作成するという指示が含まれる。「作成」要求には、複合文書サーバがその複合文書にどのスプレッドシート・オブジェクトを組み込めばいいかわかるように、スプレッドシート・オブジェクト・リファレンスも含まれる。最後に「作成」要求には、複合文書へのアクセスを要求する本人の代理として動作するオブジェクトがその複合文書へのアクセスを許可されているかどうかを複合文書サーバが判断することができるように、選択されたグループ識別子が含まれる。

【００４３】複合文書サーバは複合文書を作成し、スプレッドシート・オブジェクト・リファレンスをその複合文書に格納する（ステップ３１１）。複合文書サーバ・オブジェクト１１９は次に、クライアント・オブジェクト１１７に複合文書オブジェクト・リファレンスを送る（ステップ３１３）。第２の実施形態では、複合文書オブジェクト・リファレンスはグループ識別子と、グループ内のアクセス権を示す項目と、複合文書の識別子と、複合文書リファレンスの作成時に複合文書サーバによって生成された暗号チェックサムとを含む。

【００４４】後のある時点で、クライアント・オブジェクトは複合文書サーバに印刷要求を送る（ステップ３１５）。「印刷」要求は、複合文書リファレンスとクライアントの本人の識別標識を複合文書サーバに渡す。クライアントは任意の周知の認証機構を使用して、クライアントの本人の代理として動作する権利を有することを複合文書サーバに対して証明する（ステップ３１７）。このようにして、複合文書サーバはどの複合文書を印刷すべきかを把握し、以下で詳述するように暗号チェックサムを使用して、クライアント・オブジェクト１１７が複合文書を印刷する許可を持っていることを検証することができる。

【００４５】複合文書を印刷するために、複合文書サーバはスプレッドシート・オブジェクトに関連づけられたデータを持っている必要がある。したがって、複合文書サーバはスプレッドシート・サーバに「データ入手」要求を送る（ステップ３１９）。「データ入手」要求にはスプレッドシート・オブジェクト・リファレンスが含まれ、スプレッド・サーバがそこからデータを取り出すべきスプレッドシート・オブジェクトを知ることができるようになっている。「データ入手」要求には、複合文書サーバがその代理として動作する本人の識別標識も含まれる。

【００４６】スプレッドシート・サーバは複合文書サーバを認証する（ステップ３２１）。出願人の第２の実施形態のこの態様を実施するには、本人を認証する任意の周知の技法を使用することができる。複合文書サーバの認証が成功すると、スプレッドシート・サーバは、複合文書サーバがスプレッドシート・オブジェクトからデータを検索することができるアクセス権を持っているかどうかを判断しようとする（ステップ３２３）。アクセス権を判断するために、スプレッドシート・サーバはスプレッドシート・オブジェクト・リファレンスに付随するグループ識別子を検索する。次にスプレッドシート・サーバは、スプレッドシート・オブジェクト・リファレンスからスプレッドシート識別子を取り出す。最後に、スプレッドシート・サーバは取り出した情報を、承認された本人がスプレッドシート・オブジェクトへのアクセス権を持つ識別されたグループのメンバーであるかどうかを判断するよう求める要求と共にメンバーシップ機構１２３に送る。出願人の第２の実施形態のこの態様を実施するためには、グループ・メンバーシップを検査する任意の周知の機構を使用することができる。

【００４７】複合文書サーバの認証済み本人が指定されたグループのメンバーである場合、スプレッドシート・

サーバは、複合文書がスプレッドシート・オブジェクトにアクセスすることを許可されていることを確認するためにさらに他の検査を行う。スプレッドシート・サーバは、スプレッドシート・オブジェクト・リファレンスから暗号チェックサムを取り出して、スプレッドシート・オブジェクトの暗号チェックサムを再計算する（ステップ３２５）。次に、スプレッドシート・サーバは取り出したチェックサムを再計算したチェックサムと比較する（ステップ３２７）チェックサムが一致する場合、スプレッドシート・サーバは、オブジェクト・リファレンス内のアクセス権を条件として、複合文書サーバがスプレッドシート・オブジェクトから必要なデータを取り出すのを許可する。

【００４８】スプレッドシート・データが取り出されると、複合文書サーバはその複合文書データを印刷のために印刷サーバに送る（ステップ３２９）。

【００４９】第２の実施形態の利点の１つは、どのグループがオブジェクト・リファレンスを使用することを許可されているか、また、そのグループ内に他のどのようなメンバーが入っているかに関する状態を維持することによって、クライアント・オブジェクトは、そのグループに関連するオブジェクト・リファレンスをグループ内の別の本人に渡すことができ、その際サーバとのメッセージ交換を行わなくても済むことである。スプレッドシート・サーバとのこのような対話を省くことによって、パフォーマンスと効率が向上する。

【００５０】変更

本明細書では、例示のために特定の実施形態について説明したが、本発明の精神および範囲から逸脱することなく様々な変更を加えることができる。したがって、本発明は上記で説明した実施形態に限定されない。

【００５１】たとえば、当業者によって広く理解されている技法に従って２つの実施形態を変更することができる、いくつかの方法がある。第１の実施形態では、グループ識別子をオブジェクトに格納することができるだけでなく、オブジェクト・リファレンスを指針としてクライアントに送ることもできる。オブジェクト・リファレンスを第２のクライアントに渡す場合に、この指針を使用してサーバとのメッセージ交換を迂回することができる。第１のクライアントは、第２のクライアントがグループに入っていることを確認することができるようになる。この指針がなければ、第１のクライアントはサーバからグループ識別子を要求しなければならず、それにはメッセージ交換を必要とする。

【００５２】第２の実施形態では、オブジェクト・リファレンスが使用のために提示されたときに、サーバはオブジェクト・リファレンスをオブジェクトと共にキャッシュすることもできる。それ以降に提示されたとき、サーバはクライアントによって送られたオブジェクト・リファレンスをキャッシュ内のオブジェクト・リファレンスと照合することができる。これは、そのオブジェクト・リファレンスが同じグループ内の別のクライアントから提示された場合、サーバは暗号チェックサムを再計算する必要がないことを意味し、それによってそのアクセスについてサーバによる計算が減少し、したがってそのパフォーマンスが向上することになる。

【図面の簡単な説明】

【図１】　本発明の好ましい実施形態を実施するためのコンピュータ・システムのブロック図である。

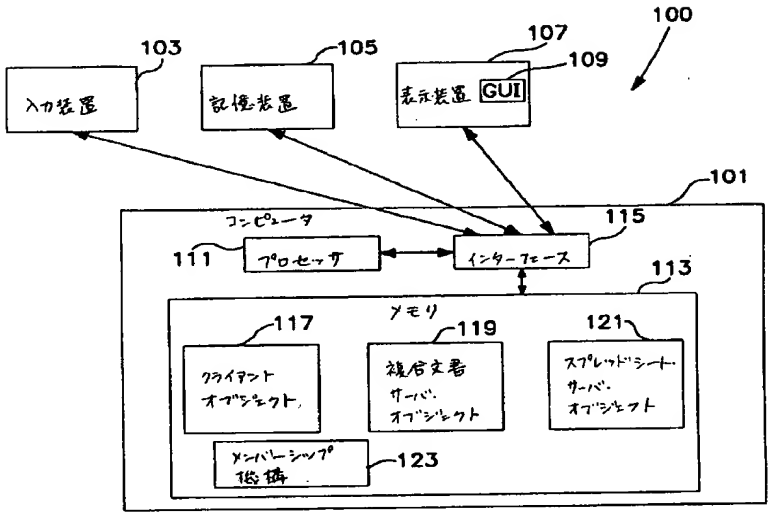
【図２】　システム資源へのアクセスを安全に制御する第１の実施形態の好ましいステップを示す流れ図である。

【図３】　システム資源へのアクセスを安全に制御する第２の実施形態の好ましいステップを示す流れ図である。

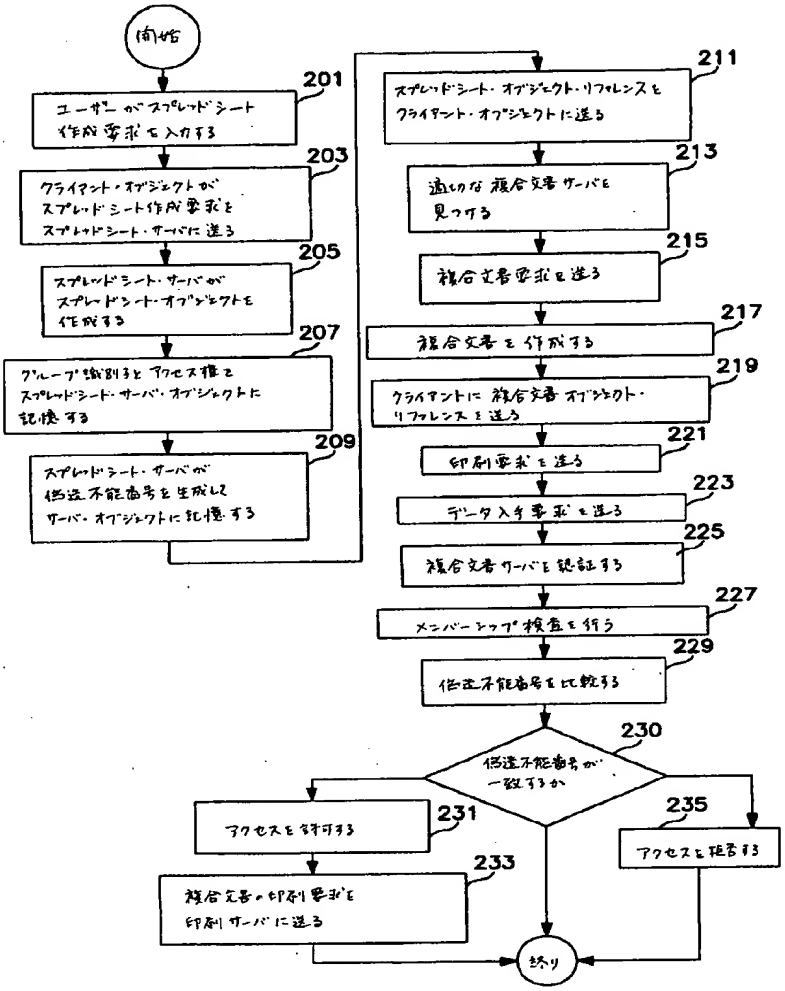
【符号の説明】

１００　コンピュータ・システム
１０１　コンピュータ
１０３　入力装置
１０５　記憶装置
１０７　表示装置
１０９　グラフィカル・ユーザ・インタフェース
１１１　プロセッサ
１１３　メモリ
１１５　インタフェース
１１７　クライアント・オブジェクト
１１９　複合文書サーバ・オブジェクト
１２１　スプレッドシート・サーバ・オブジェクト
１２３　メンバーシップ機構

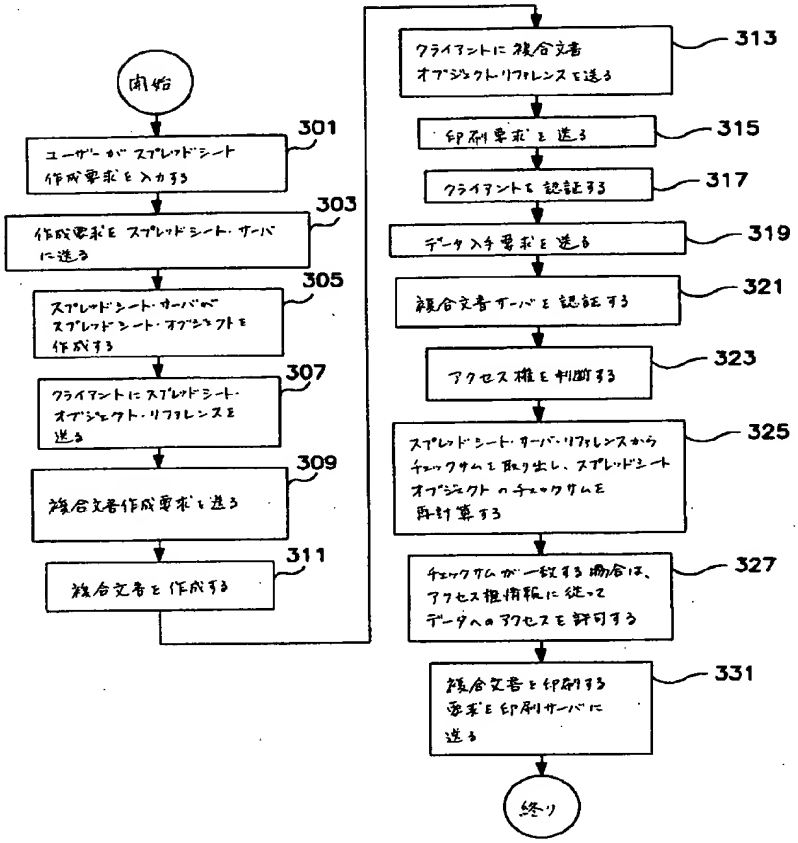
【図１】


100
103
105
107
109
入力装置
記憶装置
表示装置
GUI
101
コンピュータ
115
111
プロセッサ
インターフェース
113
メモリ
117
119
121
クライアント
オブジェクト
複合文書
サーバ・
オブジェクト
スプレッドシート
サーバ・
オブジェクト
メンバーシップ
台帳
123

【図２】


開始
201
ユーザーがスプレッドシート作成要求を入力する
203
クライアント・オブジェクトがスプレッドシート作成要求をスプレッドシート・サーバに送る
205
スプレッドシート・サーバがスプレッドシート・オブジェクトを作成する
207
グループ識別子とアクセス権をスプレッドシート・サーバ・オブジェクトに記憶する
209
スプレッドシート・サーバが偽造不能番号を生成しサーバ・オブジェクトに記憶する
211
スプレッドシート・オブジェクト・リファレンスをクライアント・オブジェクトに送る
213
適切な複合文書サーバを見つける
215
複合文書要求を送る
217
複合文書を作成する
219
クライアントに複合文書オブジェクト・リファレンスを送る
221
印刷要求を送る
223
データ入手要求を送る
225
複合文書サーバを認証する
227
メンバーシップ検査を行う
229
偽造不能番号を比較する
230
偽造不能番号が一致するか
231
アクセスを許可する
233
複合文書の印刷要求を印刷サーバに送る
235
アクセスを拒否する
終り

【図３】




---

フロントページの続き

| (51)Int.Cl.[6] | | 識別記号 | 庁内整理番号 | FI | | 技術表示箇所 |
|---|---|---|---|---|---|---|
| G09C | 1/00 | 660 | | G06F | 15/20 | 570D |
| H04L | 9/32 | | | | | 596B |
| | | | | H04L | 9/00 | 675Z |

(72)発明者　セロン・ディ・トック
アメリカ合衆国　94086　カリフォルニア州・サニーヴェイル・アヴェイラ　ドライブ・ナンバー100・1260